

Microsoft 365
対応パック



Microsoft 365対応パック 設定参考資料

私たちはMicrosoft 365をご利用中のお客様をヒアリングし、監視のニーズ/要望があり特に重要と思われるものをALog用の標準テンプレートとしました。

このテンプレートを活用することで、日常に内在する不正アクセスの発見はもちろん、拡大するサイバー攻撃の脅威に対して、素早く、効率的な検知体制が整え、その運用を自動化することが可能となります。

本書はこのテンプレートについての用途や概要をまとめた紹介資料となります。

貴社のセキュリティ強化の一助となれば幸いです。



ファイルアクセス

- ・共有リンク（匿名リンク、セキュリティで保護されたリンク）によるデータ共有
- ・ファイルアクセス（移動/コピー/削除/復元）
- ・ファイルのダウンロード/アップロード監視
- ・ファイル/フォルダ/サイトの共有監視
- ・業務時間外のファイルアクセス
- ・職場のグローバルIP以外からのファイルアクセス
- ・組織外ユーザーによるファイルアクセス/ダウンロード
- ・公開フォルダへのファイルコピー



メール

- ・メールボックスへのサインイン
- ・代理送信機能を使ったメール送付
- ・大量メール送信の検出
- ・検疫/スパムメールの受信者集計
- ・大容量ファイルのメール送信検知
- ・DLP（データ漏洩防止）検出
- ・メール送信失敗
- ・転送設定の変更検知



AD認証/管理者操作

- ・グループへのメンバー追加、グループからのメンバー削除
- ・グループの作成/削除
- ・ユーザーアカウントの作成/削除
- ・パスワードの再設定（リセット）
- ・組織外ユーザーの作成/削除、グループへの追加
- ・職場のグローバルIP以外からのログイン
- ・大量ログイン失敗
- ・業務時間外のログイン
- ・その他のAD管理イベント



チャット

- ・TEAMSへのサインイン
- ・チームの作成/変更/削除
- ・チャネルの追加/変更/削除

共有リンク（匿名リンク、セキュリティで保護されたリンク）による外部とのデータ共有

匿名リンクやセキュリティで保護されたリンクを含め、外部とのデータ共有を検知できます。
外部とのデータ共有をチェックすることで、設定の不備や許可されていないデータ共有を早期に発見でき、情報漏えいのリスクを軽減できます。

条件1

操作 共有リンク系操作を指定

Operation [対象とする] AND OR

- SharingInvitationCreated
- SharingInvitationAccepted
- SharingInvitationBlocked
- SharingInvitationUpdated
- SharingInvitationRevoked
- SecureLinkCreated
- AnonymousLinkCreated
- AnonymousLinkUpdated
- AddedToSecureLink

[除外する] AND OR

複数指定する場合、改行区切りで入力します。

UserType [対象とする] AND OR

- *(0)*
- *(2)*

ファイルアクセス（移動/コピー/削除/復元）

クラウド上のファイル操作はログを残すべきです。
特に大量のファイル移動やコピーなど漏えいに繋がるリスクが高い操作はレポーティングし、流失の形跡がないかなど追跡調査することが必要です。

条件1

操作 ファイルアクセス関連操作を指定

Operation [対象とする] AND OR

- FileMoved
- FileCopied
- FileDeleted
- FileRestored

[除外する] AND OR

複数指定する場合、改行区切りで入力します。

しきい値 しきい値を指定

+ 100 -

しきい値の間隔 1時間

ファイルダウンロード/アップロード監視

ファイルのダウンロードやアップロードは、情報漏えいにつながるリスクが高いため、しっかり監視すべきです。

「いつ、だれが、どのファイルを持ち出したのか」、「機密情報をアップロードしたのは誰か」などを把握することは、問題の拡大を未然に防ぐことに繋がります。

条件1

操作

Operation [対象とする]

☐ FileUploaded

☐ FileDownloaded

[除外する]

複数指定する場合、改行区切りで入力します。

ファイル/フォルダ/サイトの共有

不適切な情報が、不適切なメンバーに共有されていないかをチェックしたり、密かに共有フォルダを作り、本来の保管ルールを破っていないかなどを監視できます。

特に社外メンバーとの情報共有はシビアにチェックすべきです。

条件1

操作

Operation [対象とする]

☐ SharingSet

[除外する]

複数指定する場合、改行区切りで入力します。

操作一覧

☐ 0365_SHAREPOINT_SHARING

合計 1件 (1ページ中 1ページ目を表示中)

< 1 >

☒ 0365_SHAREPOINT_SHARING

業務時間外のファイルアクセス

業務時間外のファイルアクセスを監視します。深夜時間帯などのアクセスは意図していない不正アクセスの可能性もあり、定常的なモニタリングが必要です。

また時間外作業を行っている従業員の可視化にも有効です。

SharePointへのファイル関連操作を指定

操作一覧

検索: O365_SHAREPOINT_FILE_FOLDER

合計 1件 (1ページ中 1ページ目を表示中)

1 selected

操作一覧

☒ O365_SHAREPOINT_FILE_FOLD
ER (6)

[除外する]

複数指定する場合、改行区切りで入力します。

時間帯: 20:00 - 7:59

時間帯を指定

職場のグローバルIP以外からのファイルアクセス

利便性や業務効率化を優先する為、Microsoft365を導入したものの「許可していない環境からのファイルアクセスは適宜監視したい」といったニーズに対応可能です。本来アクセスすべきではない環境からのファイルアクセスを監視する事で不正の早期発見に繋がります。

SharePointへのファイル関連操作を指定

条件1

操作: 1 selected

ClientIP [対象とする]

複数指定する場合、改行区切りで入力

[除外する]

218.44.111.111

☒ O365_SHAREPOINT_FILE_FOLD
ER (6)

AND OR

職場のグローバルIPを除外

組織外ユーザーによるファイルアクセス/ダウンロード

Microsoft365上に保管されているファイルに対し、組織外ユーザーがアクセスしたり、ファイルをダウンロードしたログを検出します。外部ユーザーが不適切なファイルへアクセスしたり、持ち出していないかを確認する際に役立てることができます。

条件1

操作 **ファイルアクセス系操作を指定**

Operation [対象とする] AND OR

- FileAccessed
- FileDownloaded
- FileSyncDownloaded*
- FileDeleted*

[除外する] AND OR

複数指定する場合、改行区切りで入力します。

UserType [対象とする] AND OR

- *(0)*
- *(2)*

[除外する] AND OR

複数指定する場合、改行区切りで入力します。

ユーザー [対象とする] AND OR

- *#ext#*

外部ユーザーの意味である「#ext#」を指定

公開フォルダへのファイルコピー

公開フォルダへコピーされたファイルを確認できます。社外秘情報を不注意もしくは意図的に公開していないかチェックする際に役立てることができます。

条件1

操作 **コピーや移動操作を指定**

Operation [対象とする] AND OR

- FileCopied
- FolderCopied
- FileMoved
- FolderMoved

[除外する] AND OR

複数指定する場合、改行区切りで入力します。

UserType [対象とする] AND OR

- *(0)*
- *(2)*

[除外する] AND OR

複数指定する場合、改行区切りで入力します。

SourceRelativeUri [対象とする] AND OR

公開フォルダを入力

[除外する] AND OR

複数指定する場合、改行区切りで入力します。

グループへのメンバー追加、 グループからのメンバー削除

ユーザーがグループへ追加されたログを検出します。不適切なユーザや人事異動を伴わないグループへの追加は、関係部署への確認が必要です。

条件1

操作

グループへの追加/削除操作を指定

Operation

[対象とする]

AND OR

add member to group.

Remove member from group.

[除外する]

AND OR

複数指定する場合、改行区切りで入力します。

UserType

[対象とする]

AND OR

(0)

(2)

グループの作成/削除

新規でグループが作成されたログを検出します。
作成されたグループが外部ユーザへの公開されている場合は、利用用途や登録されているユーザーが適切かを確認する必要があります。

条件1

操作

グループの追加/削除操作を指定

Operation

[対象とする]

AND OR

add group.

delete group.

[除外する]

AND OR

複数指定する場合、改行区切りで入力します。

UserType

[対象とする]

AND OR

(0)

(2)

ユーザーアカウントの作成/削除

管理者が認識していない状態で、アカウントの作成/削除が行われることは、重大なセキュリティリスクです。
この操作を早期に察知し、「実行アカウント」と「作成されたアカウント」に不審な動きがないかを確認することは、被害の拡大を防止するうえで重要です。

The screenshot shows the '条件1' (Condition 1) configuration page. Under the '操作' (Operation) section, the '対象とする' (Target) dropdown is set to 'Add user.' and 'Delete user.', which are highlighted with a red box. A red arrow points from the text 'アカウントの追加/削除操作を指定' (Specify account addition/deletion operation) to this box. Below this, the '除外する' (Exclude) section is empty, and a note at the bottom states '複数指定する場合、改行区切りで入力します。' (When specifying multiple, input with line breaks).

パスワードの再設定（リセット）

特権が与えられたアカウントによるパスワードリセット行為をレポートできます。
適切な申請に基づいたパスワードの再設定（リセット）か否か、異常な回数の再設定（リセット）ログが無いかを発見できます。

The screenshot shows the '条件1' (Condition 1) configuration page. Under the '操作' (Operation) section, the '対象とする' (Target) dropdown is set to 'Reset user password.', which is highlighted with a red box. A red arrow points from the text 'パスワードリセット操作を指定' (Specify password reset operation) to this box. Below this, the '除外する' (Exclude) section is empty, and a note at the bottom states '複数指定する場合、改行区切りで入力します。' (When specifying multiple, input with line breaks).

組織外ユーザーの作成/削除、グループへの追加

外部ユーザーが作成されたり、グループへ追加されたログを検出します。
許可されていない外部ユーザーの作成や、作成された外部ユーザーへの不適切なアクセス権の付与/グループへの追加がなされていないかを確認する必要があります。

条件1

操作 [対象とする] AND OR

Operation [対象とする] AND OR

add user.
delete user.
add member to group.

[除外する] AND OR

複数指定する場合、改行区切りで入力します。

対象 [対象とする] AND OR

#ext#

[除外する] AND OR

複数指定する場合、改行区切りで入力します。

UserType [対象とする]

(0)
(2)

グループへの追加/削除操作を指定

外部ユーザの意味である「#ext#」を指定

職場のグローバルIP以外からのログイン

一般的に業務で利用するクラウドサービスはIPフィルタリングによりアクセス可能なGIPを制限します。
しかし設定ミスや内部不正などにより意図しないGIPからのアクセスが可能になるケースも想定し、指定のGIP以外からのログインがないかチェックすることは重要です。

Azure ADへのLOGONを指定

操作一覧

0365_AAD_STS_LOGON

合計 1件 (1ページ中 1ページ目を表示中)

< 1 >

☒ 0365_AAD_STS_LOGON (15)

複数指定する場合、改行区切りで入力します。

[除外する] AND OR

218.44.111.111

職場のグローバルIPを除外

大量ログイン失敗

短時間に大量のログイン失敗が行われることは、非常に高い確率で不正アクセスの可能性があります。Azure ADへのログインチャレンジを迅速に発見することは、サイバー攻撃の早期発見に繋がります。

業務時間外のログイン

深夜時間帯などのログインは意図していない不正ログインの可能性もあり、定常的なモニタリングが必要です。また時間外作業を行っている従業員の可視化にも有効です。

その他のAD管理イベント

ライセンス変更や多要素認証設定などの管理者操作ログを監視します。管理者の操作ログを定期的にモニタリングする事で不正操作の抑止に繋がります。

操作一覧

管理者操作を指定

Q O365_AAD_ADMIN (8)

合計 1件 (1ページ中 1ページ目を表示中)

< 1 >

ected

操作一覧

Operation

[対象とする]

AND OR

複数指定する場合、改行区切りで入力します。

[除外する]

AND OR

add group.
delete group.
update group.
add member to group.
remove member from group.
add owner to group.
remove owner from group.
update user.
add user.
delete user.



UserType

[対象とする]

(0)
(2)

グループ、アカウント
作成/削除の関連操作を除外

メールボックスへのサインイン

日頃からメールボックスへのサインイン行為を監視する事で攻撃者による不正なサインインの兆候が無いを確認します。
身に覚えの無いサインインは無い、業務時間外のサインインが無い等を確認する事で、不正アクセスの早期発見に繋がります。

条件1

メールボックスへのサインイン操作を指定

操作	選択なし	操作一覧
Operation	[対象とする]	AND OR
	MailboxLogin	
	[除外する]	AND OR
複数指定する場合、改行区切りで入力します。		

代理送信機能を使ったメール送付

代理送信機能を使ったメール送付を監視します。他人のアカウントを使用し不正なメール送付が行われていないか、不要なメール送付が行われていないかを確認出来ます。

条件1

代理送信操作を指定

操作	選択なし	操作一覧
Operation	[対象とする]	AND OR
	SendOnBehalf	
	[除外する]	AND OR
複数指定する場合、改行区切りで入力します。		

大量メール送信の検出

メール送信数を集計・レポートすることで、侵入者によるアドレス帳に登録された宛先への自動送信など、フィッシング拡大メールの自動送信を検知します。

Exchangeのメール送信操作を指定

操作一覧

Q O365_MSG_外部に送信

合計 1件 (1ページ中 1ページ目を表示中) 1 selected ▼

< 1 >

条件1

☒ O365_MSG_外部に送信

しきい値 ? 100 しきい値の間隔 1日 ▼

しきい値を指定

検疫/スパムメールの受信者集計

検疫、スパムメールを集計・レポートすることで、侵入者による外部への情報流出の可能性を検知します。

Exchangeのスパムメール操作を指定

操作一覧

Q O365_MSG_スパム

合計 1件 (1ページ中 1ページ目を表示中) 1 selected ▼

< 1 >

☒ O365_MSG_スパム

円グラフ なし

選択

転送設定の変更検知

管理者権限での転送設定変更を監視することで、侵入者による外部への不正なメール転送の予兆を検知します。

ExchangeのADMIN操作を指定

操作一覧

Q O365_EXCHANGE_ADMIN (1)

合計 1件 (1ページ中 1ページ目を表示中)

< 1 >

ed

操作一覧

Operation [対象とする]

AND OR

New-InboxRule

Set-InboxRule

UpdateInboxRules

転送設定変更操作を指定

大容量ファイルのメール送信検知

メール送信バイト数を集計・レポートすることで、侵入者による外部への情報流出の可能性を検知します。

Exchangeのメール送信操作を指定

操作一覧

条件1

O365_MSG_外部に送信

合計 1件 (1ページ中 1ページ目を表示中)

< 1 >

1 selected

操作一覧

☒ O365_MSG_外部に送信

複数指定する場合、改行区切りで入力します。

[除外する]

複数指定する場合、改行区切りで入力します。

Size

右記の数値以上

30000

しきい値を指定

DLP（データ漏出防止）検出

DLPによりメールメッセージとファイルから判定された機密情報送信有無を監視することで、侵入者による機密情報の流出を検知します。

ExchangeのDLPルール操作を指定

操作一覧

検索

合計 1件 (1ページ中 1ページ目を表示中)

< 1 >

1 selected ▼

操作一覧

☒ O365_MSG_DLP ルール ☐ 円グラフ ☐ なし

参照可能ユーザー 選択

メール送信失敗

メール送信の失敗を集計・レポートすることで、侵入者による外部への情報流出の可能性を検知します。

Exchangeのメール送信失敗操作を指定

操作一覧

検索

合計 1件 (1ページ中 1ページ目を表示中)

< 1 >

1 selected ▼

操作一覧

☒ O365_MSG_失敗 ☐ 円グラフ ☐ なし

参照可能ユーザー 選択

TEAMSへのサインイン

ユーザのMicrosoft TEAMS クライアントに対するサインインを監視します。業務時間外などの不審なサインインが無いか、休暇中のユーザになりすましたサインイン等が無いかを監視できます。

条件1 メールボックスへのサインイン操作を指定

操作	選択なし	操作一覧
Operation	[対象とする] TeamsSessionStarted	AND OR
	[除外する]	AND OR
複数指定する場合、改行区切りで入力します。		

チームの作成/変更/削除、メンバーの追加

チームを作成し、メンバーを招待（追加）する行為を監視します。業務上、作成されるべきではないチームが作成されていないか、招待されるべきではないメンバーが招待されていないか等を確認し、重要情報の流出リスクが無いかを監視できます。

条件1 チームの作成/変更/削除、メンバーの追加操作を指定

操作	選択なし	操作一覧
Operation	[対象とする] TeamCreated TeamSettingChanged TeamDeleted MemberAdded	AND OR
	[除外する]	AND OR
複数指定する場合、改行区切りで入力します。		

チャネルの追加/変更/削除

チャネル設定に関する操作（追加/変更/削除）を監視します。不必要な外部ユーザの招待が無い、業務とは関係の無いチャットグループの作成が無いなども監視する事が可能です。

条件1 チャネルの追加/変更/削除操作を指定

操作 操作一覧

Operation

[対象とする]	AND	OR
ChannelAdded		<input type="checkbox"/>
ChannelSettingChanged		<input type="checkbox"/>
ChannelDeleted		<input type="checkbox"/>

[除外する] AND OR

複数指定する場合、改行区切りで入力します。



1 適用したいパックを選ぶ



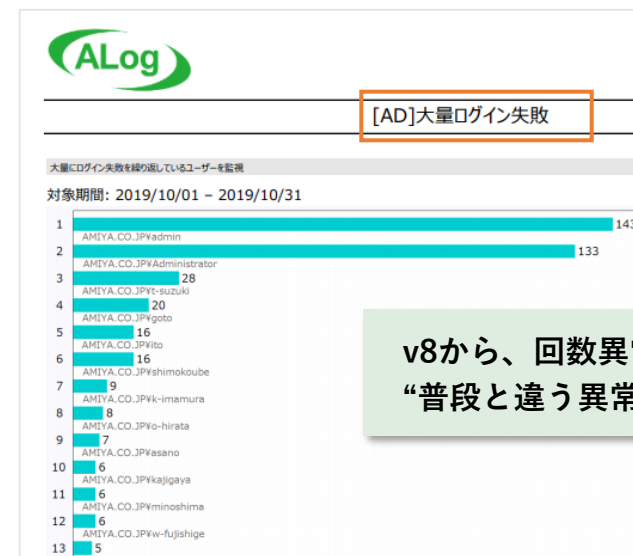
2 インポートする



3 機器名を登録したら完了



設定はこれで終了です。
あとはAIとアラートが自動検知



v8から、回数異常だけでなく
“普段と違う異常”も検知可能に